CLAIMS

WHAT IS CLAIMED IS:

1. A system for malicious code detection, comprising:

a plurality of scanning computer systems configured for scanning content for malicious code and generating an alarm when the file contains malicious code; and

a front-end processor, coupled to the scanning computer systems, configured for receiving a flow of content from an external network and distributing copies of the flow to each of the scanning computer systems in parallel for scanning; and

a detection management system, coupled to the scanning computer systems, configured for employing a countermeasure on the flow if at least one of the scanning computer systems generates the alarm.

2. The system according to claim 1, further comprising a database containing rules configured for creating a signature of a piece of malicious code detected by at least one of the scanning computer systems.

3. The system according to claim 2, further comprising a remote site detection system configured for detecting malicious code in incoming network traffic based on signatures of malicious code stored thereat.

4. The system according to claim 3, wherein the detection manager is further configured for causing the signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

5. The system according to claim 1, wherein each of the scanning computer system is configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code.

6. The system according to claim 1, wherein the flow includes at least one of a hypertext markup file and a transferred file.

7. The system according to claim 1, wherein the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code.

8. A system for malicious code detection, comprising:

a remote site detection system configured for detecting malicious code in incoming network traffic based on signatures of malicious code stored thereat;

a plurality of scanning computer systems configured to execute respective anti-virus scanning software having different, corresponding coverage of malicious code for scanning content for malicious code and generating an alarm when the content contains malicious code; and

a front-end processor, coupled to the scanning computer systems, configured for receiving a flow of content from an external network and distributing copies of the flow to each of the scanning computer systems in parallel for scanning, said flow including at least one of a hypertext markup file and a transferred file; and

a detection management system, coupled to the scanning computer systems, configured for:

creating a signature of a piece of malicious code detected by at least one of the scanning computer systems detected in the flow when at least one of the scanning computer generates an alarm on the piece of malicious code;

employing a countermeasure on the flow if at least one of the scanning computers generates an alarm on the piece of malicious code, said countermeasure including at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code; and

causing the signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

9. A method for malicious code detection in a system including a plurality of scanning computer systems, comprising:

receiving a flow of content from an external network;

distributing copies of the flow to each of the scanning computer systems in parallel;

scanning the flow for malicious code and generating an alarm when the content contains malicious code at each of the scanning computer systems; and

employing a countermeasure on the flow if at least one of the scanning computer systems generates the alarm.

10. The method according to claim 9, further comprising creating a signature of a piece of malicious code detected by at least one of the scanning computer systems.

11. The method according to claim 10, further comprising detecting malicious code in incoming network traffic at a remote site detection system based on signatures of malicious code stored thereat.

12. The method according to claim 11, further comprising updating the signatures stored at the remote site detection system to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

13. The method according to claim 9, wherein said scanning at each of the scanning computer systems includes executing respective anti-virus scanning software having different, corresponding coverage of malicious code.

14. The method according to claim 9, wherein the flow includes at least one of a hypertext markup file and a transferred file.

15. The method according to claim 9, wherein said employing the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code.

16. A method for malicious code detection in a system including a remote site detection system and a plurality of scanning computer systems, comprising:

receiving a flow of content from an external network, said flow including at least one of a hypertext markup file and a transferred file;

distributing copies of the flow to each of the scanning computer systems in parallel;

at each of the scanning computer systems, executing respective anti-virus scanning software having different, corresponding coverage of malicious code to scan the

flow for malicious code scanning and generating an alarm when the flow contains malicious code;

creating a signature of a piece of malicious code detected by at least one of the scanning computer systems detected in the flow when at least one of the scanning computers generates an alarm on the piece of malicious code;

causing signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems;

employing a countermeasure on the flow if at least one of the scanning computer generates an alarm on the piece of malicious code, including at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code; and

detecting malicious code in incoming network traffic based on the signatures of malicious code stored thereat.

17. A front-end system, coupled to an external network and a plurality of scanning computer systems, said front-end system comprising one or more processors, a communications interface, and a computer-readable medium bearing instructions for causing the one or more processors upon execution thereof to perform the steps of:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file;

duplicating the flow to produce a plurality of copies of the flow; and

distributing the copies of the flow to each of the scanning computer systems in parallel.

18. A method for operating a front-end system, coupled to an external network and a plurality of scanning computer systems, said method comprising:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file;

duplicating the flow to produce a plurality of copies of the flow; and

distributing the copies of the flow to each of the scanning computer systems in parallel.

19. A computer-readable medium bearing instructions for operating a front-end system, coupled to an external network and a plurality of scanning computer systems, said instructions arranged, when executed, for causing one or more processors to perform the steps of:

receiving a flow of content from the external network, said flow including at least one of a hypertext markup file and a transferred file;

duplicating the flow to produce a plurality of copies of the flow; and

distributing the copies of the flow to each of the scanning computer systems in parallel.

20. A malicious code detection cluster, comprising:

an internal network coupled to a front-end processor and a detection management system;

a plurality of scanning computer systems coupled to the internal network and configured for:

receiving respective copies of a flow of content from the front-end processor in parallel, said flow including at least one of a hypertext markup file and a transferred file;

executing respective anti-virus scanning software having different, corresponding coverage of malicious code to scan the respective copies of the flow in parallel for malicious code; and

transmitting an alarm to the detection management system when the flow contains malicious code as detected by at least one of the anti-virus scanning software.

21. A method of detecting malicious code in an internal network coupled to a front-end processor, a plurality of scanning computer systems, and a detection management system, said method comprising the steps of:

receiving respective copies of a flow of content from the front-end processor in parallel, said flow including at least one of a hypertext markup file and a transferred file;

executing respective anti-virus scanning software having different, corresponding coverage of malicious code to scan the respective copies of the flow in parallel for malicious code; and

transmitting an alarm to the detection management system when the flow contains malicious code as detected by at least one of the anti-virus scanning software.

22. A detection management system, coupled to a plurality of scanning computer systems, said detection management system comprising one or more processors, a communications interface, and a computer-readable medium bearing instructions arranged for causing the one or more processors upon execution thereof to perform the steps of:

receiving an alarm from one of the scanning computer systems when a flow of content scanned by the scanning computer systems in parallel contains malicious code, said flow including at least one of a hypertext markup file and a transferred file; and

employing a countermeasure on the flow if at least one of the scanning computers generates an alarm on a piece of the malicious code.

23. The detection management system according to claim 22, wherein the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code.

24. The detection management system according to claim 22, wherein the detection management system is further coupled to a remote site detection system and said instructions are further arranged for causing the one or more processors to perform the steps of:

creating a signature of a piece of malicious code detected by at least one of the scanning computer systems in the flow when at least one of the scanning computers generates an alarm on the piece of malicious code; and

causing signatures stored at the remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

25. A method of managing malicious code detection, comprising:

receiving an alarm from one of the scanning computer systems when a flow of content scanned by the scanning computer systems in parallel contains malicious code, said flow including at least one of a hypertext markup file and a transferred file; and

employing a countermeasure on the flow if at least one of the scanning computer generates an alarm on a piece of the malicious code.

26. The method according to claim 25, wherein said employing the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code.

27. The method according to claim 25, further comprising:

creating a signature of a piece of malicious code detected by at least one of the scanning computer systems in the flow when at least one of the scanning computer generates an alarm on the piece of malicious code; and

causing signatures stored at a remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.

28. A computer-readable medium bearing instructions for managing malicious code detection, said instructions arranged for causing the one or more processors upon execution thereof to perform the steps of:

receiving an alarm from one of the scanning computer systems when a flow of content scanned by the scanning computer systems in parallel contains malicious code, said flow including at least one of a hypertext markup file and a transferred file; and

employing a countermeasure on the flow if at least one of the scanning computers generates an alarm on a piece of the malicious code.

29. The computer-readable medium according to claim 28, wherein the countermeasure includes at least one of blocking the flow, quarantining the flow, and informing the recipient of the flow of the malicious code.

30. The computer-readable medium according to claim 28, wherein said instructions are further arranged for causing the one or more processors to perform the steps of:

creating a signature of a piece of malicious code detected by at least one of the scanning computer systems in the flow when at least one of the scanning computers generates an alarm on the piece of malicious code; and

causing signatures stored at a remote site detection system to be updated to include the signature of the piece of malicious code detected by said at least one of the scanning computer systems.